位相推定問題から位数計算へ

○互いに素の x、$\mathrm{M}(x < \mathrm{M})$ が与えられたとき、$x^r \bmod \mathrm{M} = 1$ を満たす最小の自然数 rを位数という

$\mathrm{U}|y\rangle = |\mathrm{xy} \bmod \mathrm{M}\rangle$ を満たす演算子Uにおいて、Uの固有状態 $|u_s\rangle$ が

$$|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{-i2\pi j\frac{s}{r}} \left|x^j \bmod \mathrm{M}\right\rangle$$

満たすとき、さらに $x^r \bmod \mathrm{M} = 1$ を満たすなら

$$\mathrm{U}|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{-i2\pi j\frac{s}{r}} \left|x^j \bmod \mathrm{M}\right\rangle = e^{i2\pi\frac{s}{r}}|u_s\rangle$$

となる。

従って位数 r は、固有値方程式 $\mathrm{U}|u_s\rangle = e^{i2\pi\frac{s}{r}}|u_s\rangle$ において位相推定問題を解くことで、求めることができる。

＜証明＞

$x^j \bmod \mathrm{M} = q$とすると、$x^j = pM + q$ と書ける。

$\mathrm{U}|y\rangle = |\mathrm{xy} \bmod \mathrm{M}\rangle$ より、

$$\mathrm{U}\left|x^j \bmod \mathrm{M}\right\rangle = \left|\mathrm{x}(x^j \bmod \mathrm{M}) \bmod \mathrm{M}\right\rangle = |\mathrm{x}\, q \bmod \mathrm{M}\rangle$$

一方、

$$\left|x^{j+1} \bmod \mathrm{M}\right\rangle = \left|x \cdot x^j \bmod \mathrm{M}\right\rangle = |x(pM + q) \bmod \mathrm{M}\rangle = |\mathrm{x}\, q \bmod \mathrm{M}\rangle$$

この２式から、

$$\mathrm{U}\left|x^j \bmod \mathrm{M}\right\rangle = \left|x^{j+1} \bmod \mathrm{M}\right\rangle$$

さらに $x^r \bmod \mathrm{M} = 1$ を用いて、

$$\mathbf{U}|\boldsymbol{u_s}\rangle = \mathrm{U}\frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{-i2\pi j\frac{s}{r}}\left|x^j \bmod \mathrm{M}\right\rangle$$

$$= \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{-i2\pi j\frac{s}{r}}\left|x^{j+1} \bmod \mathrm{M}\right\rangle$$

$$= \frac{1}{\sqrt{r}}(e^{-i2\pi\cdot 0\cdot\frac{s}{r}}|x^1 \bmod \mathrm{M}\rangle + e^{-i2\pi\cdot 1\cdot\frac{s}{r}}|x^2 \bmod \mathrm{M}\rangle + \cdots + e^{-i2\pi\cdot(\mathrm{r}-1)\cdot\frac{s}{r}}|x^r \bmod \mathrm{M}\rangle$$

$$= e^{i2\pi\frac{s}{r}}\frac{1}{\sqrt{r}}(e^{-i2\pi\cdot 1\cdot\frac{s}{r}}|x^1 \bmod \mathrm{M}\rangle + e^{-i2\pi\cdot 2\cdot\frac{s}{r}}|x^2 \bmod \mathrm{M}\rangle + \cdots + e^{-i2\pi\cdot\mathrm{r}\cdot\frac{s}{r}}|1 \bmod \mathrm{M}\rangle$$

$$= e^{i2\pi\frac{s}{r}}\frac{1}{\sqrt{r}}(e^{-i2\pi\cdot 0\cdot\frac{s}{r}}|x^0 \bmod \mathrm{M}\rangle + e^{-i2\pi\cdot 1\cdot\frac{s}{r}}|x^1 \bmod \mathrm{M}\rangle + \cdots + e^{-i2\pi\cdot(\mathrm{r}-1)\cdot\frac{s}{r}}|x^{r-1} \bmod \mathrm{M}\rangle$$

$$= e^{i2\pi\frac{s}{r}}\frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{-i2\pi j\frac{s}{r}}\left|x^j \bmod \mathrm{M}\right\rangle \quad = \quad \boldsymbol{e^{i2\pi\frac{s}{r}}|u_s\rangle}$$

（ $|x^r \bmod \mathrm{M}\rangle = |1 \bmod \mathrm{M}\rangle = |x^0 \bmod \mathrm{M}\rangle$ および $e^{-i2\pi\cdot\mathrm{r}\cdot\frac{s}{r}} = 1 = e^{-i2\pi\cdot 0\cdot\frac{s}{r}}$ を用いている。）